CLAIMS

What is claimed is:

SUB A2

1. An encryption system for the transmission of information encoded in a format using logic level transitions to derive the system clock, the system comprising;

a frame generator having a first input to accept information to be transmitted, said frame generator organizing the information into frames including both the information and system overhead, said frame generator having an output to provide frames of information to be transmitted; and

a self-synchronous scrambling circuit having an input operatively connected to the output of said frame generator, said scrambling circuit scrambling the frame input in a first predetermined encryption pattern and providing an output of encrypted frames, whereby the information to be transmitted is scrambled after it is organized into frames.

2. The encryption system of claim 1 further comprising:

a data generator having an output operatively connected to the input of said frame generator to provide information to be transmitted.

3. The encryption system of claim 1 further comprising:

a self-synchronous de-scrambling circuit having a first input operatively connected to the output of said scrambling circuit, said de-

scrambling circuit decrypting the received encrypted frames in accordance with the first encryption pattern to provide received frames of information at an output.

4. The encryption system of claim 3 further comprising:

a frame terminal having an input operatively connected to the output of said de-scrambling circuit, said frame terminal removing the overhead information associated which each frame to provide the transmitted information, whereby the transmitted information is recovered.

5. The encryption system of claim 4 further comprising:

an information terminal having a first input operatively connected to the output of said frame terminal to receive the transmitted information.

6. The encryption system of claim 4 in which said frame generator divides each frame into time multiplexed sections including a first frame period when information is included in the frame, and a second frame period when overhead is included in the frame, said frame generator having a second output to provide timing information regarding the occurrence of the first and second frame periods, and in which said scrambler having a second input operatively connected to second output of said frame generator, said scrambler selectively scrambling frame sections in response to the received frame period timing information, whereby frame sections are selectively encrypted for transmission.

7. The encryption system of claim 6 in which said scrambler encrypts only the information section of each frame in response to timing signals received from the second output of said frame generator, whereby the overhead data is not scrambled.

8. The encryption system of claim 6 in which said scrambler encrypts the information section, and selectively encrypts the overhead section of each frame in a second predetermined encryption pattern, in response to timing signals received from the second output of said frame generator, whereby the overhead data is selectively scrambled to further the transmission encryption process.

9. The encryption system of claim 6 in which said frame terminal divides each received frame into time multiplexed sections including a first frame period when information is included in the frame and a second frame period when overhead is included in the frame, said frame terminal having a second output to provide timing information regarding the occurrence of the first and second frame periods, and in which said de-scrambler has a second input operatively connected to second output of the frame terminal, said de-scrambler selectively de-scrambling frame sections in response to the received frame period timing information, whereby frame sections are selectively decrypted.

10. The encryption system of claim 9 in which said de-scrambler encrypts only the information section of each frame in response

to timing signals received from the second output of said frame terminal, whereby the overhead data is not de-scrambled.

11. The encryption system of claim 9 in which said de-scrambler decrypts the information section, and selectively decrypts the overhead section of each frame in the second predetermined decryption pattern, in response to timing signals received from the second output of said frame terminal, whereby the overhead data is selectively de-scrambled to further the transmission encryption process.

12. The encryption system of claim 9 in which said frame generator accepts packets of HDLC information, in which said frame generator organizes the information and overhead in frames according to SONET protocols, in which said frame terminal accepts information organized into frames according to SONET protocols, and in which said frame terminal supplies packets of HDLC information.

13. In a communication format using logic level transitions to derive the system clock, a method for encrypting transmissions comprising the steps of:

a) accepting information to be transmitted;

b) organizing the information into frames including time multiplexed sections of information and sections of overhead;

c) self-synchronously scrambling the frames in a first predetermined encryption pattern; and

d) transmitting the scrambled frames, whereby the information and overhead data are both encrypted for added security.

14. The method of claim 13 further comprising the steps, following Step d), of:

e) receiving the scrambled frames;

f) self-synchronously de-scrambling the frames in accordance with the first encryption pattern; and

g) recovering the information from the frames.

15. The method of claim 14 in which Step b) includes generating timing data to signal the occurrence of the information and overhead sections of the frames, and in which Step c) includes scrambling the frames in response the timing data signals of Step b).

16. The method of claim 15 in which Step g) includes generating timing data to signal the occurrence of the information and overhead sections of the received frames, and in which Step f) includes de-scrambling the received frames in response the timing data signals of Step g).

17. The method as in claim 16 in which Step c) selectively scrambling overhead sections of the frames in a second predetermined encryption pattern, and in which Step f) includes selectively de-scrambling overhead sections of the received frame in accordance with the

second encryption pattern, whereby the selective scrambling of overhead furthers the encryption process.

18. The method as in claim 15 in which Step c) includes scrambling only the information section of each frame.

19. In digital data transmission of a type that uses logic level transitions for clock recovery, a sabotage prevention system comprising:

a means for generating information;

a means for assembling the information into frames that include both the information and system overhead for transmission; and

a means for self-synchronously and continuously scrambling the frames from said assembly means, subsequent to the assembly of the frames, whereby information and overhead are encrypted for transmission.

20. The system as in claim 19 in which said self-synchronous scrambling means includes control inputs with timing data that are synchronous to at least one overhead bit in the frame to disable said scrambling means, whereby the scrambling operation becomes modifiable.